



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **07212353 A**(43) Date of publication of application: **11.08.95**

(51) Int. Cl. **H04L 9/00**
H04L 9/10
H04L 9/12
G09C 1/00

(21) Application number: **06007148**(71) Applicant: **NIPPON YUNISHISU KK**(22) Date of filing: **26.01.94**(72) Inventor: **SUDA HITOSHI**(54) **DATA COMMUNICATION SYSTEM AND DATA COMMUNICATION METHOD**

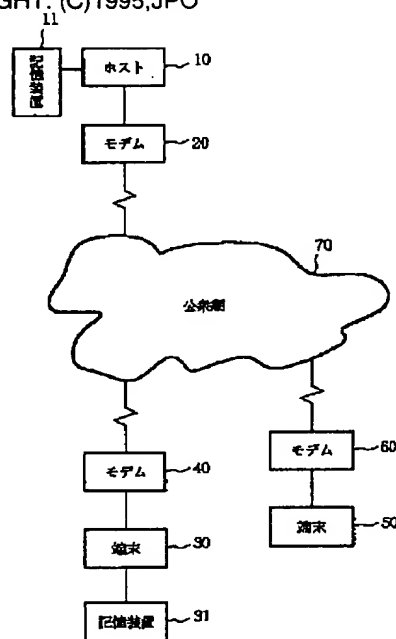
generated ASC data. When they match, a desired program is started and a desired processing is performed.

(57) Abstract:

COPYRIGHT: (C)1995,JPO

PURPOSE: To prevent an illicit access by making it possible to judge that an object to be accessed is a permitted opposite party and further changing information specifying the permitted opposite party every time an access is performed.

CONSTITUTION: When a host computer 10 responds when an access is performed from a terminal 30 to the host computer 10, the user name and the password for an illicit access prevention which are preliminarily assigned to a terminal are transmitted to the host side. The host 10 investigates whether these match with the matters registered in a storage device 11. When they match, a connection program is started, and the terminal identifier and the access sequence check data(ASC) from the terminal are received. These and the matters registered in the device 11 are compared. If they match, it is judged that the access is not illicit access, new ASC data is generated in the host 10 and the data is transmitted to the terminal 30. A ciphering processing is performed for the data, it is transmitted to the host 10, it is restored, and it is compared with the new



| | | | | |
|---------------------------|------|---------|-----|--------|
| (51) Int.Cl. ⁹ | 識別記号 | 庁内整理番号 | F I | 技術表示箇所 |
| H 0 4 L 9/00 | | | | |
| 9/10 | | | | |
| 9/12 | | | | |
| G 0 9 C 1/00 | | 9364-5L | | |

H 0 4 L 9/00 Z
 審査請求 未請求 請求項の数 4 O L (全 9 頁)

(21) 出願番号 特願平6-7148
 (22) 出願日 平成6年(1994)1月26日

(71) 出願人 591030237
 日本ユニシス株式会社
 東京都港区赤坂2丁目17番51号
 (72) 発明者 須田 仁
 東京都港区赤坂二丁目17番51号日本ユニシ
 ス株式会社内
 (74) 代理人 弁理士 大塚 康徳 (外1名)

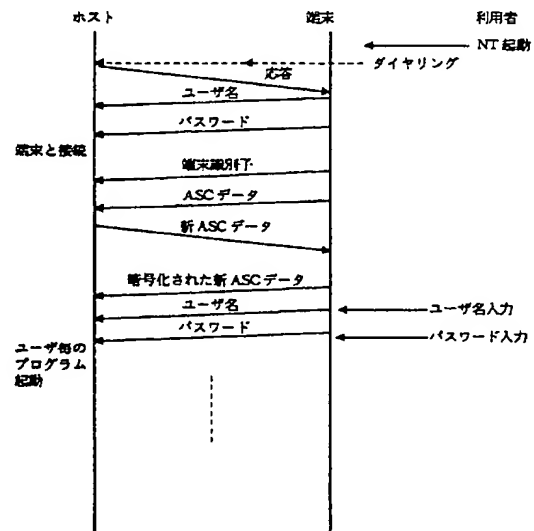
(54) 【発明の名称】 データ通信システム及びデータ通信方法

(57) 【要約】

【目的】 確実に不正アクセスを防ぐと共に例え不正アクセスがあってもこれを容易に認識可能とできるデータ通信システムを提供することを目的とする。

【構成】 端末は予め割り当てられているユーザ名及びパスワードをホストに送出しホストとの接続処理を開始する。ホストは、続いて端末より送られてくる端末に特有の端末識別子及びASCデータを受信する。そして送られてきた端末識別子及びASCデータが予め登録されているものか否かを調べ、登録されているデータであればホスト側で新たなASCデータを生成してこの更新したASCデータを端末側に送信する。そしてホスト及び端末は新たなASCデータを次のアクセス時に用いるASCデータとする。端末は、この受信した新たなASCデータに対して所定の暗号化処理を施し、暗号化ASCデータをホストに送信する。ホストはこの暗号化された新ASCデータが決められた暗号化方法により暗号化された新たなASCデータである場合には続いて端末よりユーザ名及びパスワードを送らせ所定のデータであればシステムへのアクセスを許可する。

第5図



【特許請求の範囲】

【請求項1】 通信媒体を介して複数の通信装置が互いに接続可能なデータ通信システムであって、システムに接続された少なくとも被起動側通信装置に、他の通信装置とのデータ通信を許可する前記他の通信装置毎の特定許可情報を保持する許可装置保持手段と、起動側装置よりの特定許可情報を受信する特定情報受信手段と、該特定情報受信手段で受信した特定許可情報が前記許可装置保持手段に保持された他の通信装置毎の特定許可情報に含まれるか否かを判別する判別手段と、該判別手段が受信した特定許可情報が前記許可装置保持手段に保持された他の通信装置毎の特定許可情報に含まれると判断した場合に次の通信時に通信を許可する前記起動側装置に特有の新たな特定許可情報を生成して前記起動側通信装置に送信する更新情報送信手段と、該更新手段で送信した前記起動側装置に特有の新たな特定許可情報に対して所定の暗号化方法により暗号化された暗号化特定情報を受信する暗号化特定情報受信手段と、該暗号化特定情報が前記生成した新たな特定許可情報の暗号化情報であった場合に前記起動側装置との通信を許可する通信許可手段とを備えることを特徴とするデータ通信システム。

【請求項2】 前記起動側装置に、被起動側通信装置との間でデータ通信を許可する自装置に特有の特定許可情報を保持する自装置許可情報保持手段と、通信開始時に前記自装置許可情報保持手段に保持の自装置に特有の特定許可情報を前記被起動側装置に送信する特定情報送信手段と、該特定情報送信手段での前記自装置に特有の特定許可情報を送信後に送られてくる新たな自装置に特有の前記被起動側装置による自装置との通信を許可する更新特定許可情報を受信する更新情報受信手段と、該更新情報受信手段で受信した前記更新特定許可情報を所定の暗号化方法に従って暗号化して前記被起動側装置に送信する暗号化特定情報送信手段と、前記更新情報受信手段で受信した前記更新特定許可情報を前記自装置許可情報保持手段に新たな特定許可情報として更新登録する自装置許可情報更新手段とを備えることを特徴とする請求項1記載のデータ通信システム。

【請求項3】 前記通信許可手段は、更に起動側装置よりの処理要求ユーザ名及びパスワードが送信され、かかる処理要求ユーザ名及びパスワードが予め許可された処理要求ユーザ名及びパスワードである場合に起動側装置の要求した処理の実行を許可することを特徴とする請求項1又は2のいずれかに記載のデータ通信システム。

【請求項4】 通信媒体を介して複数の通信装置が互いに接続可能なデータ通信システムにおけるデータ通信方式であって、

10

20

30

40

50

システムに接続された通信装置間で通信路を形成後に起動側通信装置より該起動側通信装置に予め登録されている被起動側通信装置との間の通信を許可する特定許可情報を送信する特定情報送信工程と、該特定情報送信工程での送信特定許可情報が前記被起動側装置に保持された通信を許可すべき他の通信装置毎の特定許可情報に含まれる場合に前記被起動側装置で新たな前記起動側装置との間の通信を許可する更新特定許可情報を生成して前記起動側通信装置に送信する更新情報送信工程と、前記起動側装置により該更新情報送信工程で送信された前記起動側装置に特有の新たな特定許可情報を次の特定許可情報として登録すると共に該更新された新たな特定許可情報に対して所定の暗号化方法により暗号化された暗号化特定許可情報を送信する暗号化特定情報送信工程とを備え、前記被起動側通信装置は該暗号化特定情報送信工程で送信された前記更新情報送信工程で送信した特定許可情報の暗号化情報である場合に前記起動側装置との通信を許可する通信許可手段とを備えることを特徴とするデータ通信方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はデータ通信システム及びデータ通信方法に関し、例えば回線網を介してデータ通信する際の不正アクセスを有効に防止可能なデータ通信システム及びデータ通信方法に関するものである。

【0002】

【従来の技術】 近年、コンピュータ関連技術が発達し、多数の情報処理装置間のデータ通信、分散処理等ができるようになってきた。これに伴い、広く誰でも利用可能な公衆回線網に接続された情報処理装置間のデータ通信等も盛んになってきており、大容量のファイルを一般ユーザがアクセスすることも可能となってきている。また、大量かつ高速処理可能なホストコンピュータを手軽にアクセスすることも可能になってきている。

【0003】 このように公衆網にシステムを開放しているシステムにおいては、基本的には誰でもシステムにアクセスすることが可能であり、システムのセキュリティを考えると非常に危険である。

【0004】

【発明が解決しようとする課題】 しかしながら、従来のこの種のシステムにおいては、システムが標準で提供しているユーザ名とパスワードによる認証システムだけに頼っている場合が多い。この認証システムではその2つのパスワードさえ知っていれば誰でもシステムに侵入することができ、また、それらのキーワードの漏洩を防ぐのは困難であるため、高いセキュリティを確保できなかった。更に、以上の認証システムではユーザ名とパスワードが漏れてシステムへの不法侵入を受けていたとして

も、この不正アクセスを認識することが困難であるという問題点もあった。

【0005】

【課題を解決するための手段】本発明は上述の課題を解決することを目的としてなされたもので、高いシステムのセキュリティを可能とすると共に、不正アクセスがあった場合においても容易にこの事実を認識可能とすることを目的とし、係る目的を達成する一手段として以下の構成を備える。

【0006】即ち、通信媒体を介して複数の通信装置が互いに接続可能なデータ通信システムであって、システムに接続された少なくとも被起動側通信装置に、他の通信装置とのデータ通信を許可する他の通信装置毎の特定許可情報を保持する許可装置保持手段と、起動側装置よりの通信装置特定許可情報を受信する特定許可情報受信手段と、該特定許可情報受信手段で受信した特定許可情報が前記許可装置保持手段に保持された他の通信装置毎の特定許可情報に含まれるか否かを判別する第1の判別手段と、該第1の判別手段が受信した特定許可情報が前記許可装置保持手段に保持された他の通信装置毎の特定許可情報に含まれると判断した場合に次回の通信時に通信を許可する前記起動側装置に特有の新たな特定許可情報を生成して前記起動側通信装置に送信する更新情報送信手段と、該更新手段で送信した前記起動側装置に特有の新たな特定許可情報に対して所定の暗号化方法により暗号化された暗号化特定許可情報を受信する暗号化特定許可情報受信手段と、該暗号化特定許可情報が前記生成した新たな特定許可情報の暗号化情報であった場合に前記起動側装置との通信を許可する通信許可手段とを備えることを特徴とする。

【0007】そして例えば前記起動側装置に、被起動側通信装置との間でデータ通信を許可する自装置に特有の特定許可情報を保持する自装置許可情報保持手段と、通信開始時に前記自装置許可情報保持手段に保持の自装置に特有の特定許可情報を前記被起動側装置に送信する特定情報送信手段と、該特定情報送信手段での前記自装置に特有の特定許可情報を送信後に送られてくる新たな自装置に特有の前記被起動側装置による自装置との通信を許可する更新特定許可情報を受信する更新情報受信手段と、該更新情報受信手段で受信した前記更新特定許可情報を所定の暗号化方法に従って暗号化して前記被起動側装置に送信する暗号化特定情報送信手段と、前記更新情報受信手段で受信した前記更新特定許可情報を前記自装置許可情報保持手段に新たな特定許可情報として更新登録する自装置許可情報更新手段とを備えることを特徴とする。

【0008】更に、例えば以下の構成を備える。即ち、前記通信許可手段は、更に起動側装置よりの処理要求ユーザ名及びパスワードが送信され、かかる処理要求ユーザ名及びパスワードが予め許可された処理要求ユーザ名

及びパスワードである場合に起動側装置の要求した処理の実行を許可することを特徴とする。

【0009】

【作用】以上の構成において、確実にシステムにアクセスしようとするものがアクセスを許可された相手であることを判断可能とし、更にアクセスの都度判断要素を変更することにより、他よりの不正アクセスを防ぐと共に例え不正アクセスがあってもこれを容易に認識可能とできる。

【0010】

【実施例】以下、図面を参照して本発明に係る一実施例を詳細に説明する。図1は本発明に係る一実施例の通信システムの構成例を示す図であり、図中、10はホストコンピュータ、11はホストコンピュータ10に備えられた記憶装置であり、この記憶装置11はホストコンピュータ10の内蔵メモリや外部記憶装置等を含んでいる。20はホストコンピュータ10を公衆網70に接続するモデムである。なお、図1では公衆網70には1つのモデム20を介して接続されている様に示しているが、このモデム20は1台に限るものではなく、アクセス頻度や処理量に応じて複数の回線を介して公衆網に接続され、該回線数分のデータ通信が可能なモデムを備える構成でもよいことは勿論である。以下では、説明の簡略化のため、ホストコンピュータ10においても接続回線数が1回線である場合を例として説明する。

【0011】30は公衆網70を介して他の通信装置、例えば、ホストコンピュータ10や他端末50等とデータ通信可能な情報処理装置である端末、31は端末30に備えられた記憶装置、40は端末30を公衆網70に接続するモデムである。更に、50は他の通信装置である端末、60は端末50を公衆網70に接続するモデム、70は公衆網であり、公衆電話回線網やISDN回線網等の汎用回線網等の誰でも容易にアクセス可能な網で構成されている。各端末においても接続回線数は任意であり、1回線に限定されるものでない。

【0012】以上の構成を備える本実施例のシステムに接続されるデータ通信を行う装置の一部構成例を図2に示す。図2に示す構成は以下に説明する本実施例におけるデータ通信に必要な部分等を選択して示した構成例であり、他の処理に必要な種々の構成を備えていることは勿論である。図2において、101は図2に示す本実施例装置全体の制御を司るCPU、102はCPU101の基本プログラムや各種基本パラメータ等を記憶するROM、103はCPU101等が実行中のプログラムの一部や処理経過等を一時記憶するRAM、104は操作者が通信装置に動作指示等を入力する操作部、105は操作指示や処理経過等を表示する表示部、106は処理結果等を入力する出力部、107は公衆網70とのインタフェースを司る回線インタフェース、120は公衆網70とのインタフェースである網制御機能を備えるモデ

ムである。なお、この通信装置が複数回線に同時接続が可能である場合には回線インタフェース107及びモデム120は同時に接続可能な回線数に対処可能である。

【0013】次に以上の構成を備える本実施例のホストコンピュータ10が備える記憶装置11のホストアクセス許可時に用いる各種情報の記憶内容の例を図3に示す。図3において、12はホストコンピュータ10の各種プログラムの実行を制御する制御プログラムやユーティリティプログラム等より成るオペレーティングシステム、13は利用者が使用する各種の目的別プログラムであるアプリケーションプログラム、14は後述するホストコンピュータ10にアクセス可能な端末情報を管理する端末管理データ部であり、端末毎に割り当てられた端末識別子15及び当該端末識別子15に対応付けて登録されている当該端末とのアクセス毎に更新される端末特定データ（特定許可情報）であるASCデータ（アクセス・シーケンス・チェック・データ）が、一対としてアクセスを許可すべき端末数分それぞれ格納されている。

【0014】また17は使用者管理データ部であり、ユーザ毎に予め割り当てられているユーザ名18及び当該ユーザ名18と対応付けて割り当てられているパスワード19が一対としてアクセスを許可すべきユーザ分だけ格納されている。なお、このASCデータはシステムで定めた桁数のチェック・データであり、本実施例では24桁の数字データで構成されている。

【0015】次に本実施例の端末（例えば端末30）が備える記憶装置31のホストアクセス時に用いる各種情報の記憶内容の例を図4に示す。図4において、32は端末30の各種プログラムの実行を制御する制御プログラムやユーティリティプログラム等より成るオペレーティングシステム、33は通信ソフトウェア（エミュレータ）であり、端末エミュレーション機能の他に端末に接続されているモデムを使用して他の通信装置との間で通信路を形成させるモデム制御機能を含んでいる。

【0016】34は端末利用者が使用する各種の目的別プログラムであるアプリケーションプログラム、35は後述するホストコンピュータ10にアクセスする際の自装置に対する端末情報を管理する端末管理データ部であり、自端末に割り当てられた端末識別子36及び自装置が次にホストコンピュータ10にアクセスする際の特定データであるASCデータ（アクセス・シーケンス・チェック・データ）が一対として格納されている。

【0017】この端末識別子36と対になっているASCデータは、正常時には図3に示すホストコンピュータ10の端末管理データ部14に格納されている端末識別子36と同じ端末識別子15に対となっているASCデータと同じ内容であり、この両者の内容が異なっている場合にはその間に誰か他の装置が不正にシステムに割り込んだことがことになる。このため、容易に不正アクセスを認識することが可能である。

【0018】なお、図4ではこの端末管理データ部35に1対のデータしか格納していないが、この端末が複数の異なる通信装置に接続可能である場合には、アクセス可能な通信装置分の端末識別子及びASCデータを格納していることは勿論である。そしてアクセスする相手装置に応じて対応する端末識別子とASCデータを使用することになる。

【0019】以上の構成を備える本実施例通信システムにおいて、公衆網70に接続されている1の通信装置（例えば端末30）より他の1の通信装置（例えばホストコンピュータ10）にアクセスし、データ通信をすべき起動をかける場合の通信制御手順を図5を参照して以下に説明する。以下の説明は公衆網70が公衆電話回線網である場合を例として説明を行う。

【0020】例えば端末30よりホストコンピュータ10にアクセスしようとする利用者は、端末30の操作部よりネットワークの起動を指示入力し、ホストコンピュータ10にアクセスする指示を入力する。この指示入力を受けた端末30のCPUは、上述した通信ソフトウェア33等を用いて回線インタフェースを介してモデム40を起動する。モデム40は回線に直流ループを形成して公衆網70に起動をかけると共に、予めホストコンピュータ10に割り当てられている電話番号に対応する電話番号信号を回線に送出してホストコンピュータ10を発呼する。

【0021】この後公衆網70は送られてくる電話番号信号で特定される発呼先（被呼側）を呼び出す。被呼側が応答すると発呼側との間で通信路を形成する。従って発呼側の端末では、被呼側であるホストコンピュータ10が応答すると、ホストコンピュータ10との間でアクセス開始プログラムを起動すべく、予め端末に割り当てられているユーザ名及び該ユーザ名に対応付けて登録されているパスワードを送出する。

【0022】このユーザ名とパスワードは、従来の通信システムで一般的に用いられている認証システムと同様のシステムが標準で提供しているユーザ名とパスワードによる認証システムである。このユーザ名とパスワードは、ここで利用者が操作部より入力する様に制御してもよいが、端末の記憶装置内に予め登録しておいたものを自動的に読み出してきてホスト側に送出するものであってもよい。本実施例の装置では以上の接続のためのユーザ名とパスワードの送信は、いわばホストコンピュータに対するログインのための、システムの不正アクセスに対するセキュリティ対策の一部を構成するのみであるため、必ずしも利用者よりの指示入力によらなければならないとする必要性が薄いためである。

【0023】このユーザ名とパスワードを受信したホストコンピュータ10は、記憶装置11に登録されているユーザ名とパスワードと合致するか否かを調べる。そして記憶装置11に登録されているユーザ名とパスワード

と一致すれば続いて本実施例に特有の端末との接続プログラムを起動する。そして続いて端末より送られてくる当該端末装置に特有の端末識別子及びASCデータを受信する。

【0024】そして記憶装置11の端末管理データ部14をアクセスして先に送られてきた端末識別子に対応付けて登録されているASCデータを読み出し、読み出してきたASCデータと続いて送られてくる端末よりの受信ASCデータとを比較する。なお、ここで、ホストコンピュータ10と端末との間の最初のデータ通信である場合には、このASCデータはシステムで決められた初期データとすることにより両通信装置間の同期が取れることになる。しかし、最初は端末の操作部より予め指示されたASCデータを指示入力するように制御してもよい。

【0025】この端末管理データ部14への登録ASCデータと端末より受信したASCデータが一致した場合には、不正アクセスではないとしてホストコンピュータ10側で新たなASCデータを生成してこの更新したASCデータを端末側に送信する。そして新たなASCデータを端末管理データ部14の端末識別子に対応したASCデータ格納領域に格納して次のアクセス時に用いるASCデータとする。

【0026】新たなASCデータ（次回に使用するASCデータ）を受信した端末は、この受信したASCデータに対して所定のホストコンピュータ10との間で取り決めた暗号化処理を施し、暗号化ASCデータをホストコンピュータ10に送信する。なお、端末側でも暗号化して新たなASCデータを送信すると共にこの暗号化前のASCデータを記憶装置31の端末管理データ部に新たなASCデータとして登録する。

【0027】この暗号化された新ASCデータを受信したホストコンピュータ10では、この暗号化ASCデータを元のASCデータに復元し、復元したASCデータと先に送った新たなASCデータとを比較する。そして両ASCデータが等しければ、続いて利用者に表示部等よりユーザ名入力を促して、操作部等よりユーザ名を入力させ、この入力されたパスワードをホストコンピュータ10に送ると共に続いて利用者にパスワードの入力を促す。そして利用者より正しいパスワードが入力されると正当にホストコンピュータ10にアクセスを許可された利用者であると判断して利用者の希望するプログラムを起動する等して所望の処理を開始する。そして所望の処理が終了すると回線を開放して一連のアクセス処理を終了する。

【0028】なお、上述の通信制御手順において、ユーザ名とパスワードの入力が使用者管理データ部17に登録されたものと異なるような場合にはその旨を報知し、所定回数、例えば3回のリトライを許容する様に制御する。以上の図5に示す通信制御手順における端末とホス

トコンピュータとの接続後ユーザ毎のプログラムが起動されるまでの本実施例に特有のセキュリティ用プログラム制御の詳細を図6及び図7のフローチャートを参照して以下に説明する。

【0029】端末よりホストコンピュータに接続のための（ホストコンピュータに対するログインのための）ユーザ名及びパスワードが送られてきてこのユーザ名及びパスワードが正しい場合には図6の処理に移行する。被呼側装置であるホストコンピュータ10は、先ずステップS1で発呼側装置であるアクセス要求端末装置に端末ID（端末識別子）を送信する様に要求する端末ID要求を送信する。そしてステップS2で端末よりの端末IDの受信を監視する。所定時間が経過しても端末IDが受信されない場合にはステップS1に戻ることになる。

【0030】ステップS51でこの端末ID要求の受信を監視していた端末側では、ホスト側よりステップS1で送信された端末IDを受信するとステップS52に進み、記憶装置31の端末管理データ部35を検索して当該発呼側装置との間で予め定められた端末識別子（36）を呼び出し、端末IDとしてホストコンピュータ10に送信する。そして続くステップS53でASCデータ要求を受信するのを監視する。所定時間が経過してもASCデータ要求が受信されない場合にはステップS51に戻ることになる。

【0031】ステップS2で端末よりステップS52で送信された端末IDが送られてくるとこれを受信してステップS3に進み、記憶装置11の端末管理データ部14を検索して送られてきた端末IDに一致する端末識別子を検索し、該当する端末識別子があれば端末側にASCデータの送信要求を送信する。そしてステップS4で相手よりのASCデータの受信を監視する。所定時間が経過してもASCデータが受信されない場合にはステップS1に戻ることになる。なお、該当する端末識別子の無い場合にはアクセスを許可されていない端末よりのアクセスである可能性が強いため図6には不図示であるが以後の処理を行わずステップS1に戻る。なお、ステップS1ではなく、不正アクセス対処処理に移行する様に制御してもよい。

【0032】端末30はステップS53でホスト側より送られてくるASCデータ要求を受信するとステップS54に進み、記憶装置31の端末管理データ部35の先に送信した端末識別子36に対応付けて登録されているASCデータを読み出し、ホストコンピュータ10に送信する。そしてステップS55で新たなASCデータの受信を監視する。所定時間が経過しても新たなASCデータが受信されない場合にはステップS51に戻ることになる。

【0033】ステップS4で端末30よりのASCデータを受信したホストコンピュータ10は、続くステップS5で記憶装置11の端末管理データ部14に格納され

10

20

30

40

50

ている先に受信した端末IDで特定される端末識別子に対応付けて登録されているASCデータと、ここで受信したASCデータとが一致するか否か（送られてきた端末ID及びASCデータが正しいデータか否か）を調べる。先に受信した端末IDで特定される端末識別子に対応付けて登録されているASCデータと、ここで受信したASCデータとが一致しない場合にはアクセスを許可されていない端末よりのアクセスである可能性が強いため以後の処理を行わずステップS1に戻る。なお、ステップS1ではなく不正アクセス対処処理に移行する様に制御してもよい。

【0034】また、この場合には他にこの間にシステムに不正アクセスがあったような場合が考えられるため、更に両者のASCデータを確認することで、不正アクセスがあったか否かを容易且つ簡単に知ることができ、迅速な対処が可能となる。これも本実施例に特有の優れた作用効果である。一方、ステップS5で先に受信した端末IDで特定される端末識別子に対応付けて登録されているASCデータと、ここで受信したASCデータとが一致する場合にはステップS6に進み、新たに次のアクセス時に使用すべきASCデータを作成する。この新たな更新ASCデータはランダムに定めた数字を用いても、所定の演算式等に基づいて求めた値としてもよい。この場合には複数の演算式を用意しておき、ランダムにこの複数の演算式の一つの演算式を選択して新たなASCデータを求める等して他の不正アクセス者が容易に特定できないようなデータとすることが望ましい。なお、ここでは所定演算式中の定数をランダムに変更するようのものであってもよい。

【0035】続いてステップS7で新たに作成したASCデータを端末側に送信すると共に、ステップS8で予め端末との間で決められているアルゴリズムに従って暗号化して例えばRAM等に一時記憶しておく。そしてステップS9で端末30より暗号化ASCデータが送られてくるのを監視する。所定時間が経過しても暗号化ASCデータが受信されない場合にはステップS1に戻ることになる。

【0036】一方、ステップS55でステップS7でホスト側より送信される新たなASCデータ（次回に使用するASCデータ）を受信した端末側では、続くステップS56で受信した新たなASCデータを記憶装置31の端末管理データ部に新たなASCデータとして登録する。これと共に、受信した新たなASCデータに対して所定のホストコンピュータ10との間で取り決めたアルゴリズムに従って暗号化処理を施し、ステップS57で暗号化ASCデータをホストコンピュータ10に送信する。そしてその後ホストコンピュータより送られてくるASC（アクセス・シーケンス・チェック）正常終了信号を受信してASC終了処理を実行し、引き続いてステップS59でエミュレータモードに移行する。

【0037】一方、ステップS9で端末側よりステップS55で送信された暗号化ASCデータを受信したホストコンピュータ10では、続くステップS10で受信した暗号化ASCデータとステップS8で暗号化したASCデータとが一致するか否かを調べる。両ASCデータが一致すればASC正常終了信号を送信してアクセスを許可を報知し、ASC終了処理を実行する。そしてステップS12に進み、端末に対してユーザ名の入力を要求する。このユーザ名の要求を受けた端末30側では、ステップS60で表示部よりユーザ名の入力要求画面を表示する。この表示部の表示を確認した利用者は、ステップS61で所定のユーザ名を操作部等より指示入力する。ユーザ名が入力されると端末30は入力されたユーザ名をホストコンピュータ10に送信する。

【0038】ステップS13でこの端末よりのユーザ名を受信したホストコンピュータ10は、記憶装置11の使用者管理データ部17を検索し、受信したユーザ名が登録されていることを確認した後ステップS14に示す様に端末側にパスワードを要求する。このパスワード要求を受けた端末側ではステップS62で表示部よりパスワードの入力要求画面を表示する。

【0039】この表示部の表示を確認した利用者は、ステップS63で所定のパスワードを操作部等より指示入力する。パスワードが入力されると端末30は入力されたパスワードをホストコンピュータ10に送信し、一連のホストコンピュータへのログイン処理を終了する。以後は利用者が所望のプログラム処理、ホストコンピュータアクセス処理を行う。

【0040】一方、ステップS15で端末よりのパスワードを受信したホストコンピュータ10は、続くステップS16で使用者管理データ部17中のユーザ名及びパスワードと一致するか否かを判断し、受信したユーザ名及びパスワードが使用者管理データ部17中のユーザ名及びパスワードと一致した場合には正当なアクセスを許可された利用者よりのアクセス要求であると判断して以下で所望の処理を行うことになる。なお、受信したユーザ名及びパスワードが使用者管理データ部17中のユーザ名及びパスワードと一致しない場合にはステップS12に戻り、以上のユーザ名及びパスワードの要求処理を所定回数、例えば3回繰り返す。この所定回数繰り返しても受信したユーザ名及びパスワードが使用者管理データ部17中のユーザ名及びパスワードと一致しない場合には不正アクセスとしてステップS1に移行、又は不正アクセス対処処理に移行する様に制御してもよい。

【0041】以上説明した様に本実施例によれば、確実にシステムをアクセスしようとするものがアクセスを許可された相手であることを判断可能とし、更にアクセスの都度ASCデータを変更することにより、他よりの不正アクセスを防ぐと共に例え不正アクセスがあってもこれを容易に認識可能とできる。

【0042】

【発明の効果】以上説明した様に本発明によれば、確実にシステムをアクセスしようとするものがアクセスを許可された相手であることを判断可能とし、更にアクセスの都度許可された相手であることを特定する情報を変更することにより、他よりの不正アクセスを防ぐと共に例え不正アクセスがあってもこれを容易に認識可能とできる。

【図面の簡単な説明】

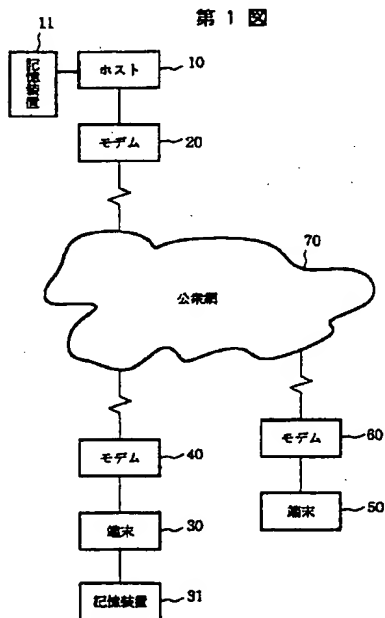
【図1】図1は本発明に係る一実施例の通信システムの構成例を示す図である。

【図2】本実施例のシステムに接続されるデータ通信を行う装置の一部構成例を示す図である。

【図3】本実施例のホストコンピュータが備える記憶装置におけるホストアクセス許可時に用いる各種情報の記憶内容の例を示す図である。

【図4】本実施例の端末が備える記憶装置におけるホストアクセス許可時に用いる各種情報の記憶内容の例を示す図である。

【図1】



【図5】本実施例のデータ通信をすべき起動をかける場合の通信制御手順を示す図である。

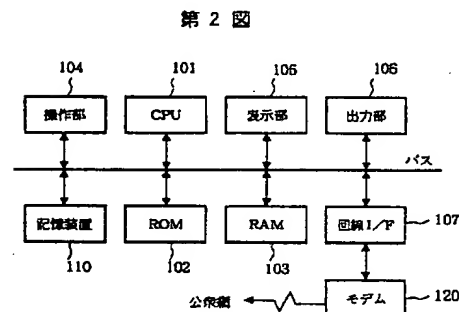
【図6】本実施例におけるアクセス開始時の制御を示すフローチャートである。

【図7】本実施例におけるアクセス開始時の制御を示すフローチャートである。

【符号の説明】

- 10 ホストコンピュータ
- 11, 31 記憶装置
- 20, 40, 60, 120 モデム
- 30, 50 端末
- 70 公衆網
- 101 CPU
- 102 ROM
- 103 RAM
- 104 操作部
- 105 表示部
- 106 出力部
- 107 回線I/F
- 107 回線インターフェース

【図2】

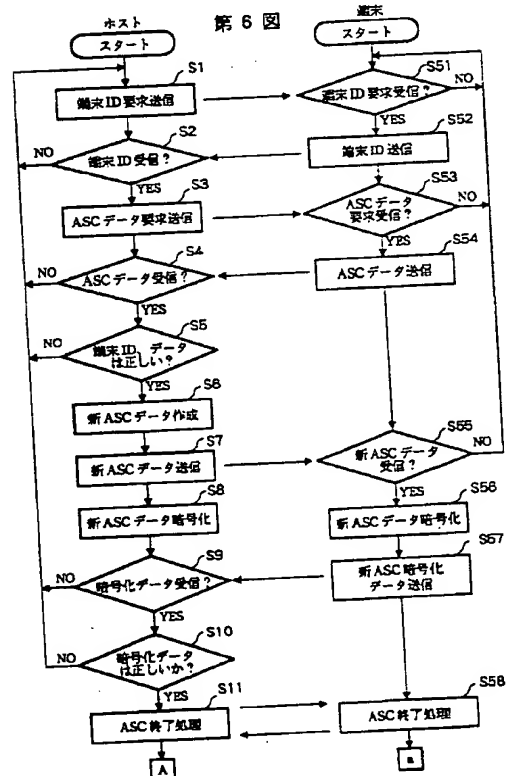


【図4】



第 5 図

The diagram illustrates the communication flow between a Host (ホスト) and a Terminal (端末). The process begins with a '利用者' (User) performing 'NT 起動' (NT Start), which leads to 'ダイヤリング' (Dialing) from the Terminal to the Host. The Host then sends a '応答' (Response) back to the Terminal. Subsequently, the Terminal sends the following data to the Host: 'ユーザ名' (Username), 'パスワード' (Password), '端末識別子' (Terminal Identifier), 'ASC データ' (ASC Data), and '新 ASC データ' (New ASC Data). The Host then sends '暗号化された新 ASC データ' (Encrypted New ASC Data) back to the Terminal. Finally, the Terminal sends 'ユーザ名入力' (Username Input) and 'パスワード入力' (Password Input) to the Host. The Host then performs 'ユーザ格のプログラム起動' (User Grid Program Start). A dashed line indicates a continuation of the process.



【図7】

第7図

